

AD-A040 328

HONEYWELL INFORMATION SYSTEMS INC MCLEAN VA FEDERAL --ETC F/G 9/2
SECURITY AND INTEGRITY PROCEDURES.(U)
JUL 76 J R GILSON

UNCLASSIFIED

ESD-TR-76-294

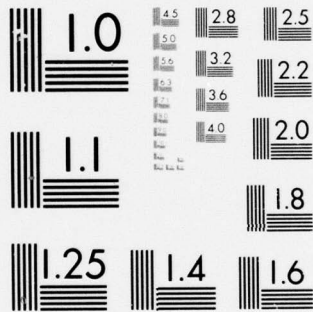
F19628-74-C-0193
NL

| OF |
AD
A040328



END

DATE
FILMED
7-77



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

12



SECURITY AND INTEGRITY PROCEDURES

Honeywell Information Systems, Inc.
Federal Systems Operations
7900 Westpark Drive
McLean, VA 22101

July 1976

Approved for Public Release;
Distribution Unlimited.

Prepared for

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
HANSCOM AIR FORCE BASE, MA 01731

AD No. 040328
DDC FILE COPY

DDC
JUN 8 1977
B

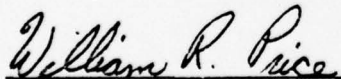
LEGAL NOTICE

When U. S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

OTHER NOTICES

Do not return this copy. Retain or destroy.

This technical report has been reviewed and is approved for publication.

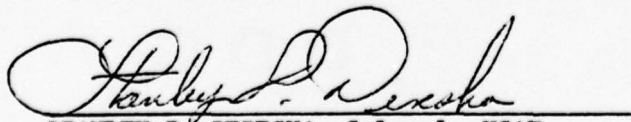


WILLIAM R. PRICE, Captain, USAF
Techniques Engineering Division



DONALD P. ERIKSEN
Techniques Engineering Division

FOR THE COMMANDER



STANLEY P. DERESKA, Colonel, USAF
Deputy Director, Computer
Systems Engineering
Deputy for Command & Management Systems

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 18 ESD-TR-76-294 19	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) 6 SECURITY AND INTEGRITY PROCEDURES	5. TYPE OF REPORT & PERIOD COVERED 9 Technical rept.	
7. AUTHOR(s) 10 J. R. Gilson	8. CONTRACT OR GRANT NUMBER(s) 15 FI9628-74-C-0193	
9. PERFORMING ORGANIZATION NAME AND ADDRESS Honeywell Information Systems, Inc. Federal Systems Operations 7900 Westpark Drive McLean, VA 22101	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS CRDL Item A014	
11. CONTROLLING OFFICE NAME AND ADDRESS Deputy for Command and Management Systems Electronic Systems Division Hanscom AFB, MA 01731	12. REPORT DATE 11 July 1976	
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	13. NUMBER OF PAGES 16 12 210	
16. DISTRIBUTION STATEMENT (of this Report) Approved for Public Release; Distribution Unlimited.	15. SECURITY CLASS. (of this report) UNCLASSIFIED	
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A	
18. SUPPLEMENTARY NOTES	<div style="text-align: right;"> HTS Write Section <input checked="" type="checkbox"/> DDC Buff Section <input type="checkbox"/> UNANNOUNCED <input type="checkbox"/> JUSTIFICATION <input type="checkbox"/> BY <input type="checkbox"/> DISTRIBUTION/AVAILABILITY CODE <input type="checkbox"/> Dist. Avail. and/or Special <input type="checkbox"/> A </div>	
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) security, security kernel, kernel, operating system, multilevel access, Multics, integrity.		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This report covers the procedures required to protect critical phases of the design, development, and certification of a secure Multics. Involved is protection of the security kernel software from unauthorized alteration or sabotage. The facilities of the Government Information Security Program are applied. The program includes protection of a security kernel for Multics and a security kernel for the Secure Communications Processor.		

P R O J E C T G U A R D I A N

SECURITY AND INTEGRITY PROCEDURES

TECHNICAL REPORT

February 16, 1977

Prepared for

Department of the Air Force
Electronic Systems Division
Hanscom Air Force Base
Bedford, Massachusetts 01731

Contract No. F19628-74-C-0193

CDRL Sequence No. A014

Honeywell Information Systems, Inc.
Federal Systems Operations
7900 Westpark Drive
McLean, Virginia 22101

PREFACE

Because of funding limitations, the Air Force terminated the effort which this document describes before the effort reached its logical conclusion. This report is incomplete but was published in the interest of capturing and disseminating the computer security technology that was available when the effort was terminated.

CONTENTS

- 1.0 Introduction
 - 1.1 Purpose
 - 1.2 Background
 - 1.3 Required Characteristics
 - 1.4 Available Tools
- 2.0 Special Considerations
 - 2.1 The Protection Problem
 - 2.2 Use of Security Classification
- 3.0 Proposed Procedures
 - 3.1 Protected Environment
 - 3.2 Verification Team
 - 3.3 Physical Site
 - 3.4 Operating Procedures
 - 3.5 Marking The Master Copies
 - 3.6 Use of the Multics Access Isolation Method
 - 3.7 Accountability and Control
 - 3.8 Transfer to Other Sites
- Appendix A Air Force Electronic System Division Comments

SECTION 1

Introduction

1.1 Purpose

This report presents a set of procedures intended to ensure the security and integrity of the final Operational Prototype Secure Multics Demonstration System produced under Project Guardian. The report first presents a brief background of the goals of the project and then considers the unusual security and integrity problems associated with this development. The threats to be countered are discussed and finally, a set of operating procedures are presented. The problem addressed by these procedures is essentially that of a trade-off between the need and desire for absolute integrity of the resulting system and the costs and operational difficulties encountered in providing the desired level of integrity.

1.2 Background

Project Guardian is part of a coordinated effort to develop the technology required to support secure multilevel computing. The primary goal of the project is development and demonstration of a multiuser resource sharing system that is capable of being certified for military use. The system must provide secure service for several levels of classified information being concurrently operated upon by users with several different levels of clearances.

The military has developed and placed in use effective means for implementing, verifying, and certifying physical, communication, and personnel security. The problem of providing an equivalent level of confidence in computer system access controls remains unsolved. A computer system with a verifiable and certifiable secure operating system is needed to complete the provision of secure computing services. This problem is being addressed by Project Guardian.

The method being used is to develop a security kernel for the operating system of a large general purpose resource sharing system and a security kernel for the communications processor that serves the large system. The security kernel has the responsibility of enforcing the access rules of the DoD Information Security Program. The design of the security kernel isolates, in one area of the system, all of the mechanisms required to ensure that the security rules are rigidly enforced. By isolating only security related functions in the kernel, the size and complexity of the kernel code is reduced to the point that formal methods of proof of correctness can be applied. Project Guardian is engaged in the development of such kernels

for the Multics operating system and for the front-end processor that connects Multics to communications lines.

The kernel design is based upon a mathematical model of a secure system. Formal proofs are used to demonstrate that the kernel, as coded in the system development language, does indeed conform to the requirements of the model. Conforming means that the kernel code performs precisely as the model indicates.

A formal process of verification of the kernels will take place. Verification means that the kernels have been technically proven to operate as documented, conforming precisely to the model and to the specifications. Verification is a technical quality control process that ensures the correct functioning of the kernel.

Formal verification of the suitability and capability of the kernel based system to enforce the security rules is the target of the technical development of Project Guardian. Before the resulting system can be used in an operational secure site, it must be examined and certified as suitable for the use intended. Certification is a process where the responsible approving authority decides that the system will indeed perform its functions as specified, that the functions performed are appropriate to the use at hand, and that the system adequately supports the security requirements of the user agency. The Air Force intends to certify the resulting kernel based Multics system for test and evaluation at an operational Air Force Multics installation.

This document addresses the requirements for protection of the Multics security kernel and the Front-End Processor security kernel in the final stages of development. The final kernel based Multics system must be verified and certified as suitable for operational use, so the kernels must be produced and verified in a reliable environment. The characteristics of the required environment and the procedures to be followed by the team that produces and verifies the kernels are discussed in later portions of this report.

1.3 Required Characteristics

A secure multilevel resource sharing system must be capable of:

- o providing computing service to a diverse community of users.
- o accommodating users with several different levels of clearance.
- o processing and storing data with several different levels of classification.

- o enforcing the Department of Defense Information Security Program Regulations.
- o being technically verified to meet the above requirements.
- o being formally certified as adequate for the specific application intended.

The Air Force has specified that an acceptable system must be secure as a result of the functioning of the hardware and software. The system cannot depend on secrecy or the hope that an antagonist does not know and understand the mechanism involved. The security kernel programs are thus to be unclassified, openly distributed to the public, and commercially available.

The overall goal of Project Guardian is to develop a secure multilevel resource sharing system that meets the above objectives. The system being developed is based on the commercially available Multics system of Honeywell Information Systems, Inc. A description of Project Guardian, and plans for the development effort, has been published. (1) An Operational Prototype Secure Multics Demonstration System is to be produced as the final output of Project Guardian. This system is then to be used in a test and evaluation situation at an operational Air Force Multics site. This system may also be used as a reliable source for transfer of the system to other Multics sites.

The Operational Prototype Secure Multics Demonstration System is expected to be used in a real situation, processing operational secure (classified) information. Therefore, it is essential that the system be reliable, verifiable, and certifiable for such use. The Statement of Work for Project Guardian places the following requirement on the development effort:

Since the security kernel is fundamental to the protection of highly classified data, it is important that the kernel be protected from sabotage during the development process. One example of sabotage is the insertion of trapdoors in the kernel code. Security procedures shall therefore be developed for the general protection of the kernel during the development process. The contractor and the Air Force shall work together to identify a set of procedures describing the clearance requirements for the personnel and physical environment involved in the protection, development, and certification of the security kernel.

(1) "Multics Security Integration Requirements", Honeywell Information Systems, Inc., to be published as an ESD Technical Report.

The Air Force has further advised Honeywell that the security level of the kernel software verification effort may not have to be as high as the security level of the data which will be processed by the kernel based system. However, it is necessary that the security level of the verification effort be sufficient so that users with the highest clearance will entrust their classified data to the kernel. Discussion of the appropriate security level to be used and of the procedures to be followed in kernel development is the subject of this document.

There are many steps in the development of a security kernel and many documents and versions involved. Among the documents that must be protected are the master specifications for the kernels, the representations of the kernel source code, and the object code of the kernel itself. Most of these materials will exist in both machine readable form and in human readable form. The threat to be counteracted is any form of unauthorized modification of any of these master representations. There is no threat of disclosure, since it is the intent of the project to publish the results openly.

The possible mechanisms for unauthorized modification include the planting of Trojan Horse procedures, trapdoors, or loopholes in any of the materials used for the development and verification process. Such modifications could conceivably be placed in the material at any level with the result that an unknown and undetected vulnerability might be built into the system for exploitation at some later date.

Another mechanism for unauthorized modification centers on the hardware used to support the development effort. A modification, trapdoor, or bypass might be installed in the computer system hardware used to verify the kernel. Such a modification might be used to mask the presence of a security flaw, preserving it for later exploitation.

Thus, both the hardware system used for the development and the master development materials need to be protected to provide the degree of confidence required for acceptance of the resulting kernel based Multics system.

1.4 Available Tools

There are a number of tools and procedures available to provide the required degree of protection. These include the provisions of the DoD Information Security Program, the use of the Access Isolation Mechanism of Multics, and configuration management.

Examination of the available tools and procedures has led to the conclusion that only use of the DoD Information Security Program, with its attendant clearances, classifications, and formally defined procedures, provides the degree of confidence needed to

ensure acceptance of the kernel based system for its intended use. Only the Information Security Program provides a set of enforceable criteria for admittance to the group of people authorized to create and modify the master materials. Only the Information Security Program provides the set of formally defined and legally enforceable procedures for the handling of the master material. Finally, only the Information Security Program provides the set of enforceable legal constraints and penalties to ensure compliance with the procedures to be followed.

The Access Isolation Mechanism of Multics provides a set of capabilities that can be used to support the requirements of the Information Security Program. The Access Isolation Mechanism is an implementation of the rules of the Information Security Program within the Multics system, providing enforcement of the security rules in the operation of Multics. However, the Access Isolation Mechanism alone is not sufficient to supply the protection required. It can enforce the security rules only within the confines of the Multics system. Other mechanisms are required for enforcement outside of the Multics system.

Configuration Management is a set of formal disciplines designed to ensure that items produced under its control conform to the approved specifications. The discipline of Configuration Management will be used to control changes and modifications to the kernels, particularly after the close of the verification phase of activity. (1)

The Information Security Program provides three levels of protection, CONFIDENTIAL, SECRET, and TOP SECRET. Considering the intended use of the Operational Prototype Secure Multics Demonstration System, the use of the TOP SECRET level of protection appears necessary. The Air Force may desire to increase the level of protection of the material by assigning one or more special access categories as well as the designation TOP SECRET. This does not initially appear to be required.

The Information Security Program is described and specified by a number of Department of Defense, and Air Force publications. The principal publications used to specify this program are:

(1) "Configuration Management Plan", Honeywell Information Systems, Inc., ESD-TR-76-354.

DoD 5200.1-R Information Security Program Regulation
DoD 5220.22-M Industrial Security Manual for Safeguarding
Classified Information
AFR 205-1 Information Security Program

SECTION 2

Special Considerations

2.1 The Protection Problem

The master material to be protected from unauthorized modification includes both human and machine readable representations of information. It is essential to the integrity of the verification and certification process that there be a guaranteed one-to-one correspondence between the human readable and the machine readable representation of a particular piece of information. Only the master copies of the material need such protection. One of the requirements of the project (no dependence on secrecy) means that unauthorized disclosure of the material is no threat and requires no protection. The master materials must be protected from unauthorized alteration at the security level desired for the final kernel based system. In Multics access control terms, the problem is one of giving read access to everyone while restricting write and modify access to a very small and select group. The difficulty comes from the many ways that a sufficiently motivated malicious person may find to subvert the controls imposed.

Use of the procedures of the Information Security Program provides the degree and kind of protection needed, but such use also provides protection that is not needed. The Information Security Program was designed to protect sensitive material from unauthorized disclosure as well as to protect it from unauthorized alteration. This project does not require protection from disclosure, so many of the procedures of the Information Security Program are not required. In particular, there is no requirement to shield the computer hardware to prevent electromagnetic radiation.

2.2 Use of Security Classification

The Information Security Program encourages classification of the least material possible at the lowest level practical. The lowest acceptable level appears to be TOP SECRET since the resulting kernel based system may well find its way into the most sensitive usage areas of the government. The least material to be classified appears to be the master copies of the items used to specify, code, and run the Multics kernel and the Front End Processor Kernel.

The material to be protected will be selected and specified by agreement between the Air Force and Honeywell. It is likely that the source programs (written in the system development language) for both the Multics security kernel and the Front End Processor security kernel will be protected. Similarly, the object code

for the two kernels requires protection. Other items that may be considered for protection include both the machine readable and human readable representations of the mathematical model, the top level kernel specification, the system specification, the kernel development specifications, and the kernel product specifications.

The material is eligible for the protection of classification under the Information Security Program, DoD 5200.1-R. Paragraph 2-303, Specific Classifying Criteria, lists two items met by Project Guardian as criteria for classification. These are:

- (a) The information provides the United States, in comparison with other nations, with a scientific, engineering, technical, operational, intelligence, strategic or tactical advantage directly related to the national security.
- (e) There is sound reason to believe that knowledge of the information would: (a) provide a foreign nation with an insight into the war potential or the war or defense plans or posture of the United States; (b) allow a foreign nation to develop, improve or refine a similar item of war potential; (c) provide a foreign nation with a base upon which to develop effective counter measures; (d) weaken or nullify the effectiveness of a defense or military plan, operation, project or activity which is vital to the national security.

The possession of a certifiable secure multilevel system will provide the United States with an operational advantage and markedly reduce the expense of secure computing.

Access to the protected master representations could provide a foreign power with a base for effective countermeasures through sabotage and unauthorized modification to the kernels. This could weaken or nullify the effectiveness of the kernel based Multics system as a means of protecting military information which is vital to the national security.

Honeywell recommends use of the Information Security Program and classification to protect the kernels under final development and verification. Only the Air Force can make the determination that this degree of protection is warranted. The formal requirements for such determination are outlined in the referenced regulations (DoD 5200.1-R and AFR 205-1) in Paragraph 2-403, "Research, Development, Test and Evaluation Programs".

SECTION 3

Proposed Procedures

3.1 Protected Environment

It is recommended that a protected environment be established for the performance of the final security kernel development, verification, and demonstration. This protected environment shall be as appropriate for material and activities at the TOP SECRET classification. Variations from the requirements of a standard TOP SECRET closed area will be discussed below in conjunction with the components of the environment and the personnel involved.

3.2 Verification Team

A standard part of the Information Security Program is the restriction of access to the minimum number of people and the granting of security clearances to only those people who require access to the material. In accordance with this well established principle, it is recommended that a Verification Team be established. The Verification Team shall consist of the smallest number of people practical to perform the functions required in the development, verification, and demonstration of the Operational Prototype Secure Multics Demonstration System.

All members of the Verification Team must possess security clearances of at least the protection level chosen for the development. Within the Verification Team, only those with specific need for write and modify access on the master materials shall be given need-to-know access. Need-to-know access shall be restricted to the specific master material concerned and be valid only for the time period required to perform the specific task.

One member of the Verification Team shall be designated as System Security Administrator with responsibility for granting, monitoring, and removing need-to-know access privileges.

The support personnel at the site must also possess adequate security clearances. These personnel include machine operators, clerical support personnel, computer maintenance engineers, and building maintenance personnel.

3.3 Physical Site

The physical site used for the protected portion of the kernel development effort shall be protected at the level selected for the development. Closed Areas shall be established for the office space for the Verification Team, for the protected

terminals used to access the computer, for the computer system used, and for the storage of the protected master material. Provisions of the Information Security Program, as detailed in the Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M) shall be followed in preparing these areas. Specific waivers of requirements may be requested to avoid unnecessary operational restrictions and expense. Since the Information Security Program was designed primarily for prevention of disclosure of information, there will be numerous requirements that provide protection from threats which are not of concern here.

The working area for the Verification Team shall be designated as a Closed Area as defined by Paragraph 34, "Area Controls", and Appendix V, "Guidelines for the Physical Construction of Closed Areas", of the Industrial Security Manual. The purpose of this designation is to reduce the opportunity for unauthorized individuals to access the protected master materials and to influence the contents of the materials.

The computer hardware used to provide Multics service and to support the demonstration system shall be housed in a Closed Area. This is to ensure that only individuals with the proper level of clearance, or individuals escorted by personnel with the proper clearance, can gain access to the hardware used for the project. The threat of unauthorized modification of the hardware system used is countered by this designation. This Closed Area may not require the full protection specified for the chosen level of protection, since unauthorized disclosure of information is not a threat.

A Closed Area shall be established to house the terminals used by the Verification Team to access the computer hardware. These terminals shall be attached to the computer by hardwired lines which are protected at the same level as the rest of the system.

A storage facility for the protected master materials shall be established. This facility must meet the requirements of Paragraph 14, "Storage", and Appendix IV, "Outline Construction Specifications for Storage Vaults", of the Industrial Security Manual. Both human readable (paper) and machine readable (magnetic tapes or disks) representations of the protected master copies must be kept in the storage facility. The storage facility will be used to hold the protected master copies of the material when they are not in use. The storage facility completes the physical protection capability required for protection of the master material.

3.4 Operating Procedures

Detailed operating procedures will be established for the portion of the effort that is to be performed under protection. These procedures will be based upon the requirements of the Information Security Program as detailed in the Industrial Security Manual and applicable Air Force Regulations. The procedures will be administered by the designated System Security Administrator. The detailed operating procedures will be based upon these guidelines:

1. The master copy of each item is protected by being classified at the selected level, probably TOP SECRET.
2. Master copies are marked in distinctive fashion in accordance with the rules given in the Information Security Program and related Air Force Regulations.
3. All other representations and copies of the material are not protected and are designated UNCLASSIFIED. No special markings are required.
4. The master copy of an item is kept under strict accountability control. It is serial numbered and registered upon creation and is logged in a master control station. All access to the master copy is recorded at the control station.
5. Superseded master copies will be destroyed according to the selected level of protection. A minimum number of history copies, all clearly designated as such, will be maintained.
6. Only those members of the Verification Team who have "need-to-know" granted by the System Security Administrator will have access to write on or modify the master copy.
7. Only those members of the Verification Team who have "need-to-know" granted by the System Security Administrator will be allowed to generate a new master copy. Generation includes assembly, compilation, linking, printing, or machine editing.
8. The System Security Administrator will grant "need-to-know" access only to those with legitimate requirements for such access and only for the time periods necessary for the completion of the functions.
9. All other activities of the Verification Team and the uncleared system developers will be carried out using unprotected copies of the material.

10. The act of transferring information from an unprotected source to the protected master copy will be done with the full knowledge and responsibility that this is the critical act in the entire process. Appropriate safeguards, including distribution of effort, checking, and personal signature acknowledgement will be applied.

3.5 Marking the Master Copies

The master copy of each item is protected by classification while other, nonmaster copies are unclassified. The master copy must be distinctly marked in accordance with the requirements of the Industrial Security Manual for material of the selected level. Both human readable representations (printed on paper) and machine readable representations (held in the Multics virtual memory or residing on magnetic tape or disk) must be marked.

Paper copies shall be stamped with the classification level on the front and back. Each master copy produced shall have a serial number assigned to it. A Data Accountability Form will also be generated for use as a receipt when the master copy is accessed by anyone. The creation, access, and disposition of each master copy shall be recorded at a Master Control Station. Capabilities of the Multics Access Isolation Mechanism (AIM) may be used to mark the classification on the pages and to generate the Data Accountability Form when the document is printed.

Machine readable copies shall be handled in a manner similar to that used for paper copies. Magnetic media containing representations of a master copy shall be marked on the media and on the container with a label showing the level of protection and a serial number for the media. Data Accountability Forms and Master Control Station logging will be used for the control of magnetic media.

While a representation of a master copy is residing in the virtual memory of Multics, the system shall be operated in accordance with the regulations of the Industrial Security Manual. The system shall be operated as a protected system whenever it contains a representation of the protected master kernel and it is expected that this representation will be written out and reused as a representation of the master.

3.6 Use of the Multics Access Isolation Mechanism

The Access Isolation Mechanism (AIM) provides a computer based implementation of the DoD Information Security Program, but is not a full kernel based system and so is not certifiable to the level desired for this program. AIM does provide a large set of control capabilities to augment the protection of the master copies. The Access Isolation Mechanism can be used on Multics to

provide the desired protection and isolation of machine readable representations of the master materials.

AIM provides sensitivity levels, special access categories, and need-to-know controls that are under the control of the System Security Administrator. The System Security Administrator can limit the access capabilities of persons, projects, and terminal devices. An Audit Log is maintained that records selected items of security interest as the system is used. AIM also provides for the automatic marking of the sensitivity level on printer output and for the generation of a Data Accountability Form for each item of protected information printed.

The System Security Administrator can designate a protected copy of each service program that will be used in the editing or creation of a master copy. For example, a particular copy of the compiler can be designated as protected, with access for its use restricted, to those members of the Verification Team with "need-to-know". All compilations of master material can then be done using this protected version of the compiler. This will reduce the possibility of unknowns being introduced by way of sabotage of the service programs. Service programs which are candidates for such protection include the text editor, system programming language compiler, linker, and the debugging tools used.

3.7 Accountability and Control

The Information Security Program (DoD 5200.1-R) and the Air Force Regulation that expands it (AFR 205-1) detail the handling requirements for material protected at the TOP SECRET level. Paragraph 7-300 in both references describes the requirement for a Top Secret Control Officer (TSCO), who is the System Security Administrator referenced earlier. The Master Control Station uses a log called the "Top Secret Register" for accountability registration and document control.

It is recommended that the procedures given in Paragraph 7-300 be followed for this phase of the development effort.

3.8 Transfer to Other Sites

When it is desired to transfer the Operational Prototype Secure Multics Demonstration System to another physical site, the need for protection remains. It is recommended that a protected copy of the kernels be produced and transferred to the destination as a classified shipment. Once the new kernel is safely within the destination, it may be declassified if desired. The rationale for this method of transfer is to extend protection from the protected source kernel to the new destination kernel. The protection subsequently given the new kernel is the prerogative

of the using organization. It will depend on the use made of the Multics system at the new site and on the security environment at the new site.

APPENDIX A

Air Force Electronic System Division Comments

Section 1.2 -- Incorporate reference to other Honeywell, Mitre and Air Force documents which describe the efforts and results alluded to by this section.

Page 6, line-11 (eleventh line from bottom of page) -- Unclassified is also a security level.

Page 15 -- Add a conclusion to this report.